PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-134310

(43)Date of publication of application : 20.05.1997

(51)Int.Cl. G06F 12/14
G06F 3/06

(21)Application number : 07-288930

(22)Date of filing : 07.11.1995

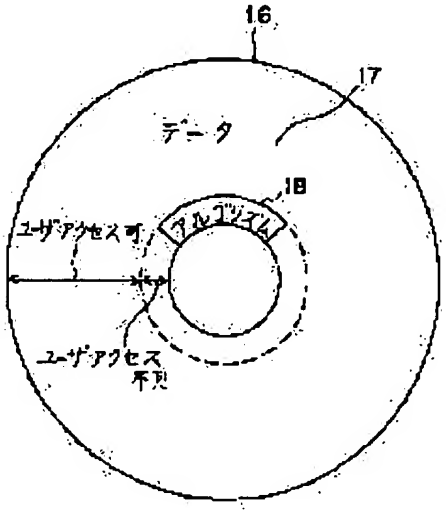
(71)Applicant : FUJITSU LTD

(72)Inventor : MASUDA TATSURO
KANEMOTO KOICHI
MURAKAMI KEIICHI
YOSHIOKA MAKOTO
KOTANI MASATAKE
YOSHIMOTO SHINICHI
FUJIWARA MASAO

(54) STORAGE MEDIUM AND METHOD FOR STORING DATA DECODING ALGORITHM

(57)Abstract:

PROBLEM TO BE SOLVED: To highly guarantee the security of ciphered data stored in a storage medium.
SOLUTION: Ciphered data 17 are stored in an area prepared in a storage medium 16 and allowed to be accessed by a user program and decoding algorithm for the data 17 is stored in an area not to be accessed by a user. A drive device loaded with the storage medium 16 extracts the algorithm 18 and decodes the data in accordance with the description of the algorithm 18. Since the data and its decoding algorithm are combined as a pair, a different ciphering method can be used in each data.



LEGAL STATUS

[Date of request for examination] 24.03.2000

[Date of sending the examiner's decision of rejection]	28.06.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	2005-14331
[Date of requesting appeal against examiner's decision of rejection]	27.07.2005
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－134310

(43)公開日　平成９年(1997)５月20日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	12/14	３２０		Ｃ０６Ｆ	12/14	３２０Ｂ
	3/06	３０４			3/06	３０４Ｈ

審査請求　未請求　請求項の数11　ＯＬ　（全６頁）

(21)出願番号　特願平7－288930

(22)出願日　平成７年(1995)11月７日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　増田　達朗
群馬県前橋市問屋町１丁目８番３号　株式会社富士通ターミナルシステムズ内

(72)発明者　金元　浩一
群馬県前橋市問屋町１丁目８番３号　株式会社富士通ターミナルシステムズ内

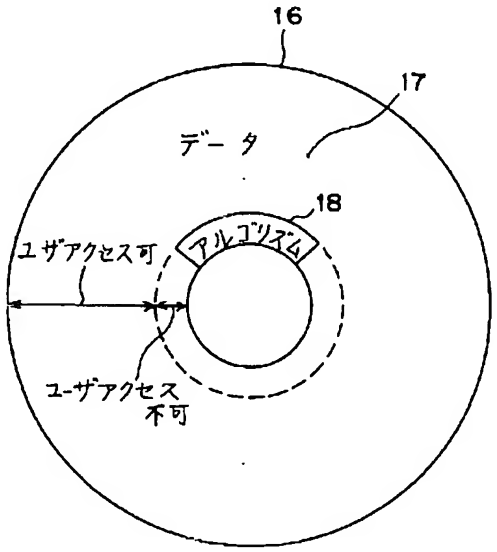
(74)代理人　弁理士　大菅　義之　（外１名）

最終頁に続く

(54)【発明の名称】　データの復号アルゴリズムを記憶する記憶媒体および方法

(57)【要約】
【課題】　記憶媒体に格納された暗号化されたデータのセキュリティを高度に保証することを課題とする。
【解決手段】　記憶媒体１６内のユーザプログラムによるアクセスが可能な領域にはデータ１７が暗号化されて格納され、ユーザによるアクセスが不可能な領域にはデータ１７の復号アルゴリズム１８が格納される。記憶媒体１６を装着されたドライブ装置はアルゴリズム１８を取り出し、その記述にしたがってデータ１７を復号する。データとその復号アルゴリズムがペアになっているので、データ毎に異なる暗号化方法を用いることができる。

媒体の記憶領域を示す図



【特許請求の範囲】
【請求項１】　暗号化されたデータを有するデータ領域手段と、
該データを復号するためのアルゴリズムを有するアルゴリズム領域手段とを備えることを特徴とする記憶媒体。
【請求項２】　前記データ領域手段は、前記記憶媒体中のユーザによるアクセスが可能な部分に設けられ、前記アルゴリズム領域手段は、該記憶媒体中のユーザによるアクセスが禁止された部分に設けられることを特徴とする請求項１記載の記憶媒体。
【請求項３】　データを有するデータ領域手段と、
該データにアクセスするためのアルゴリズムを有するアルゴリズム領域手段とを備えることを特徴とする記憶媒体。
【請求項４】　前記データ領域手段は、前記記憶媒体中のユーザによるアクセスが可能な部分に設けられ、前記アルゴリズム領域手段は、該記憶媒体中のユーザによるアクセスが禁止された部分に設けられることを特徴とする請求項３記載の記憶媒体。
【請求項５】　暗号化されたデータと、該データを復号するためのアルゴリズムとを有する記憶媒体を装着する手段と、
前記記憶媒体から前記データとアルゴリズムを取り出し、該アルゴリズムに従って該データを復号する復号手段とを備えることを特徴とする復号装置。
【請求項６】　記憶媒体から取り出された、暗号化されたデータと該データを復号するためのアルゴリズムとを受け取る手段と、
前記アルゴリズムに従って前記データを復号する復号手段とを備えることを特徴とする復号装置。
【請求項７】　記憶媒体から取り出された、暗号化されたデータと該データを復号するための暗号化されたアルゴリズムとを受け取る手段と、
前記アルゴリズムの復号を外部装置に依頼し、復号されたアルゴリズムを受け取り、該復号されたアルゴリズムに従って前記データを復号する復号手段とを備えることを特徴とする復号装置。
【請求項８】　暗号化されたデータと該データを復号するためのアルゴリズムとをペアにして記憶することを特徴とする記憶方法。
【請求項９】　暗号化されたデータと該データにアクセスするためのアルゴリズムとをペアにして記憶することを特徴とする記憶方法。
【請求項１０】　暗号化されたデータと、該データを復号するためのアルゴリズムとを有する記憶媒体から、該データとアルゴリズムを取り出し、
前記アルゴリズムに従って前記データを復号することを特徴とする復号方法。
【請求項１１】　記憶媒体から取り出された、暗号化されたデータと該データを復号するためのアルゴリズムとを受け取り、
前記アルゴリズムに従って前記データを復号することを特徴とする復号方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、記録されたデータのセキュリティを保証する記憶媒体とその記憶方法、および暗号化されたデータの復号装置とその復号方法に関する。
【０００２】
【従来の技術】情報処理技術の分野において、情報を記録する記憶媒体にはいくつかの種類のものがある。従来より用いられている記憶媒体としては、磁気テープ、磁気ディスク、光磁気ディスク、光ディスク等が知られており、今日ではますます多様化する傾向にある。このような記憶媒体に記録される情報には秘密性の高いものがあり、それらは暗号化されて記憶されることが多い。
【０００３】例えば、磁気ディスク内の暗号化情報を復号する従来の情報処理システムでは、ドライブ装置に装着されたディスクから暗号化されたデータを読み出し、あらかじめ決められた復号アルゴリズムを用いてそれを復号している。復号アルゴリズムが与えられていない他のシステムではデータを解読することができず、ディスクのセキュリティが保証される。
【０００４】
【発明が解決しようとする課題】しかしながら、上述のような従来のセキュリティ保証方法には次のような問題がある。
【０００５】ディスク内のデータを復号するアルゴリズムがシステムで固有になっているため、一旦そのアルゴリズムが解読されると、他のシステムでも同じアルゴリズムを使用してデータを読むことができるようになる。
【０００６】また、システムが保持する復号アルゴリズムに適応するような暗号化ディスクを作成するために、ディスク作成者にそのアルゴリズムを公開する必要がある。このため、第３者が公開されたアルゴリズムを手に入れて、暗号を解読する可能性がある。
【０００７】このように復号アルゴリズムが単一であるため、それが何等かの方法で一旦破られると、暗号化されたデータのセキュリティが保証されないという問題がある。
【０００８】本発明は、暗号化されたデータのセキュリティを高度に保証することのできる記憶媒体とその記憶方法を提供することを目的とする。
【０００９】
【課題を解決するための手段】図１は、本発明の記憶媒体の原理図である。図１の記憶媒体１は、暗号化されたデータを有するデータ領域手段２と、そのデータを復号するためのアルゴリズムを有するアルゴリズム領域手段３とを備える。

【００１０】データとその復号アルゴリズムがペアにして同一の媒体中に格納されるので、データ毎または媒体毎に異なる暗号化方法および復号方法を適用することが可能になる。このため、あるデータの復号アルゴリズムが第３者に知られた場合でも、それにより他のデータを復号することはできず、大多数のデータのセキュリティが守られることになる。

【００１１】また、データ領域手段２は、記憶媒体１中のユーザによるアクセスが可能な部分に設けられ、アルゴリズム領域手段３は、記憶媒体１中のユーザによるアクセスが禁止された部分に設けられる。

【００１２】このように、アルゴリズム領域手段３に対するユーザによるアクセスを禁止することで、その中に格納された復号アルゴリズムがユーザに知られる危険性を低くすることができる。この場合、データ領域手段２内のデータは簡単に取り出すことができるが、その暗号解読方法が取り出せないため、データのセキュリティが保証される。

【００１３】また、データ領域手段２がデータを有し、アルゴリズム領域手段３がそのデータにアクセスするためのアルゴリズムを有するように構成することもできる。この場合も、データとそのアクセスアルゴリズムがペアにして同一の媒体中に格納され、データ毎または媒体毎に異なるアクセス方法を適用することが可能になる。したがって、データのセキュリティが高くなる。

【００１４】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態を詳細に説明する。図２は、本発明の記憶媒体を用いる第１の実施形態の情報処理システムの構成図である。図２の情報処理システムは、パーソナルコンピュータ（ＰＣ）１１とドライブ装置１２を備える。

【００１５】ドライブ装置１２は、復号部１４とローダ１５を有する復号機構１３を備え、装着された媒体１６から暗号化されたデータ１７とその復号アルゴリズム１８を読み出す。復号部１４は、ＰＣ１１から与えられたキーとローダ１５から受け取ったアルゴリズム１８を用いてデータ１７を復号し、その結果をＰＣ１１に渡す。

【００１６】復号機構１３は、例えば、ドライブ装置１２に備えられたマイクロ・プロセッサ等の処理装置により実現される。また、アルゴリズム１８は、暗号解析方法や媒体１６へのアクセス方法を含み、復号機構１３が理解することのできる中間言語で記述されている。

【００１７】図３は、媒体１６の記憶領域の例を示している。図３の媒体１６は、例えば、磁気ディスク、光ディスク、光磁気ディスク等であり、円形のディスク状の形をしている。ユーザによるアクセスが可能な領域にはデータ１７が暗号化されて格納されており、ユーザによるアクセスが不可能な領域にはアルゴリズム１８が格納されている。ここで、ユーザによるアクセスとは、ユーザのアプリケーション・プログラムがデバイスドライバ等のソフトウェアを介して行うアクセスを意味する。ただし、ドライブ装置１２はユーザアクセスが不可能な領域にもアクセスすることができる。

【００１８】図４は、復号機構１３によるデータの復号処理のフローチャートである。図４において処理が開始されると、復号機構１３は、まずＰＣ１１からデータ１７のリード要求とともに暗号解読用のキーを受け取る（ステップＳ１）。次に、ローダ１５が媒体１６中のアルゴリズム１８をロードして復号部１４に渡す（ステップＳ２）。

【００１９】次に、復号部１４が媒体１６中のデータ１７を読み出し（ステップＳ３）、アルゴリズム１８に従い、キーを用いてデータ１７を復号する（ステップＳ４）。このとき、例えば、アルゴリズム１８に定められたデータ変換式中の変数にキーを代入して、データ１７の変換を行う。そして、復号されたデータをＰＣ１１に渡して（ステップＳ５）、処理を終了する。

【００２０】このように、アルゴリズム１８はユーザからは参照することができず、ドライブ装置１２の内部だけで使用されるので、アルゴリズム１８自身の秘密性が高度に保持される。ユーザがアルゴリズム１８を参照できないということは、暗号化されたデータ１７のコピーを作ることはできても、媒体１６のコピーは作れないことを意味する。したがって、データ１７のセキュリティが保証される。

【００２１】また、データ１７とアルゴリズム１８をペアにして媒体１６に格納するので、データ毎にまたは媒体毎に異なる復号アルゴリズムを採用することができる。したがって、万が一アルゴリズムが漏れるようなことがあっても、それを用いて他の媒体のデータを解読することはできない。

【００２２】第１の実施形態では、ドライブ装置１２の内部でデータ１７の復号を行っているが、これをその外部で行うことも可能である。図５は、データ１７の復号をＰＣ１１内で行う第２の実施形態の情報処理システムの構成図である。図５において、基本的に図２と同様の構成要素には同じ符号が付けられている。

【００２３】図５のＰＣ１１内では、アプリケーション・プログラム２１が外部のドライブ装置１２にアクセスする際に、アクセス専用のソフトウェアツールであるデバイスドライバ２２を用いる。デバイスドライバ２２は復号部２３とローダ２４を備え、図２の復号機構１３と同様の役割を果たす。したがって、デバイスドライバ２２によるデータ１７の復号処理のフローは、基本的に図４と同様である。

【００２４】ただし、この場合、復号部２３は、ステップＳ１においてアプリケーション・プログラム２１からリード要求とキーを受け取り、ステップＳ３においてドライブ装置１２からデータ１７を受け取り、ステップＳ５においてアプリケーション・プログラム２１にデータ

を渡す。また、ローダ２４は、ステップＳ２においてドライブ装置１２からアルゴリズム１８をロードする。

【００２５】第２の実施形態においても、アルゴリズム１８はアプリケーション・プログラム２１から参照することができず、アルゴリズム１８およびデータ１７のセキュリティが保証される。

【００２６】図６は、暗号化されたアルゴリズムを有する媒体を解読する第３の実施形態の情報処理システムの構成図である。図６において、基本的に図５と同様の構成要素には同じ符号が付けられている。

【００２７】図６の情報処理システムは、通信ネットワーク３２を介してＰＣ１１に結合した他の計算機であるサーバ３３を備える。また、ドライブ装置１２には、データ１７とともに暗号化されたアルゴリズム３４を格納する媒体３５が装着される。デバイスドライバ２２内のローダ３１はアルゴリズム３４をＰＣ１１内にロードした後、サーバ３３にそれを送り、アルゴリズム３４の復号を依頼する。そして、サーバ３３が復号したアルゴリズムを受け取り、それを復号部２３に渡す。復号部２３は、渡されたアルゴリズムに従って、データ１７を復号する。

【００２８】図７は、図６のデバイスドライバ２２によるデータの復号処理のフローチャートである。図７において処理が開始されると、デバイスドライバ２２は、まずアプリケーション・プログラム２１からデータ１７のリード要求とともにデータ１７の暗号解読用のキーを受け取る（ステップＳ１１）。

【００２９】次に、ローダ３１がドライブ装置１２から媒体３５中のアルゴリズム３４をロードする（ステップＳ１２）。そして、ネットワーク３２を介して、アルゴリズム３４の復号をサーバ３３に依頼し（ステップＳ１３）、サーバ３３から復号されたアルゴリズムを受け取って、復号部２３に渡す（ステップＳ１４）。

【００３０】次に、復号部２３が媒体３５中のデータ１７を読み出し（ステップＳ１５）、復号されたアルゴリズムに従い、キーを用いてデータ１７を復号する（ステップＳ１６）。そして、復号されたデータをアプリケーション・プログラム２１に渡して（ステップＳ１７）、処理を終了する。

【００３１】第３の実施形態によれば、復号アルゴリズム３４そのものも暗号化されるので、媒体３５のセキュリティはさらに高くなる。また、アルゴリズム３４を解読するためのアルゴリズムはサーバ３３に保持されているため、第３者は容易に知ることができない。

【００３２】

【発明の効果】本発明によれば、暗号化されたデータとその復号アルゴリズムをペアにして記憶媒体に格納するため、データ毎にまたは媒体毎に異なる暗号化アルゴリズムを採用することができる。

【００３３】また、ユーザは記憶媒体中の復号アルゴリズムにアクセスすることができないので、媒体全体をコピーすることができない。したがって、媒体中のデータのセキュリティが高くなる。

【図面の簡単な説明】

【図１】本発明の原理図である。

【図２】第１の実施形態の構成図である。

【図３】媒体の記憶領域を示す図である。

【図４】復号機構の処理のフローチャートである。

【図５】第２の実施形態の構成図である。

【図６】第３の実施形態の構成図である。

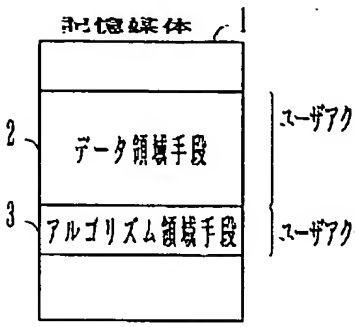
【図７】デバイスドライバの処理のフローチャートである。

【符号の説明】

１、１６、３５　記憶媒体
２　データ領域手段
３　アルゴリズム領域手段
１１　パーソナルコンピュータ
１２　ドライブ装置
１３　復号機構
１４、２３　復号部
１５、２４、３１　ローダ
１７　データ
１８、３４　アルゴリズム
２１　アプリケーション・プログラム
２２　デバイスドライバ
３２　ネットワーク
３３　サーバ

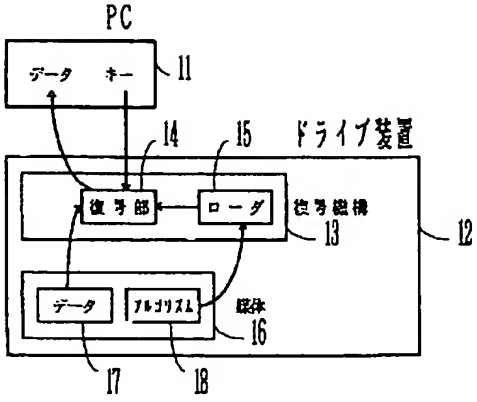
【図1】

本発明の原理図



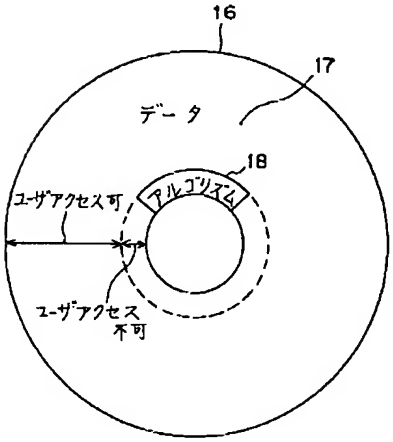
【図2】

第1の実施形態の構成図



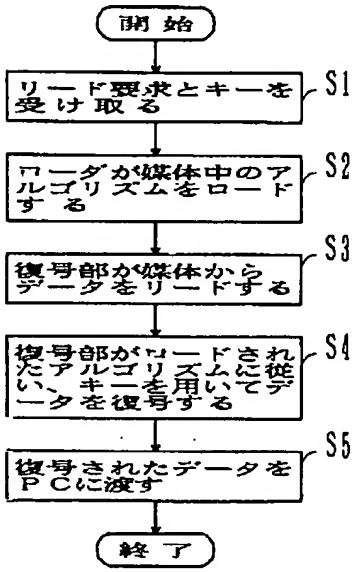
【図3】

媒体の記憶領域を示す図



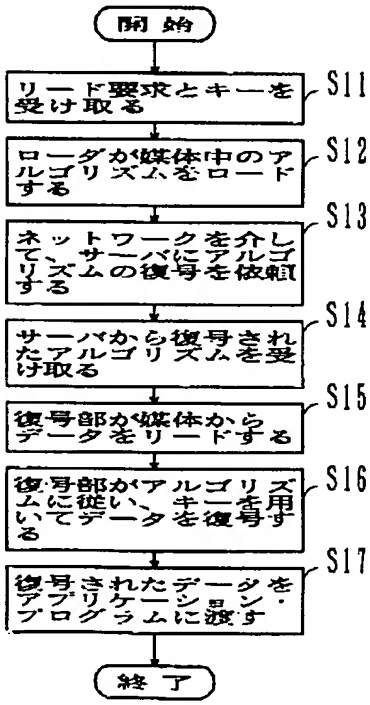
【図4】

復号機構の処理のフローチャート



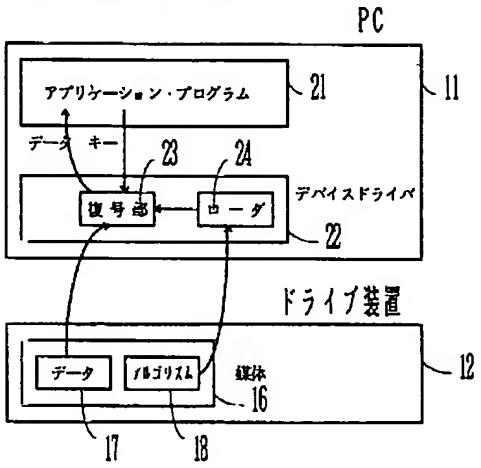
【図7】

デバイスドライバの処理のフローチャート



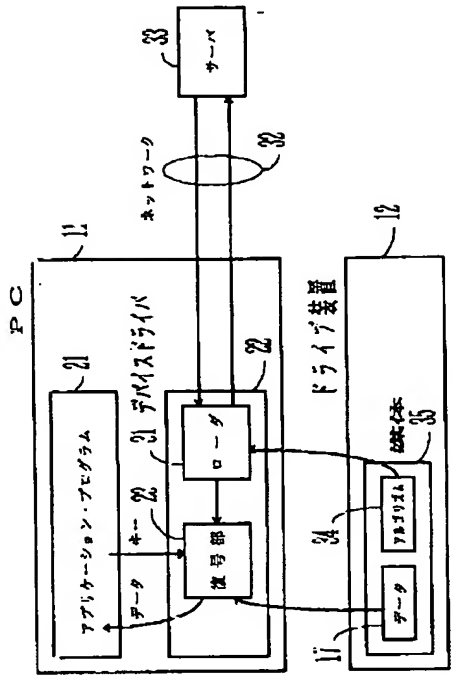
【図5】

第２の実施形態の構成図



【図6】

第３の実施形態の構成図



フロントページの続き

(72)発明者　村上　敬一
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　吉岡　誠
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　吉本　真一
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　藤原　眞雄
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内